DEPARTMENT OF STATE
PRIVACY IMPACT ASSESSMENT

May 2008

Global Financial Services Charleston
Document Imaging System
(DIS)

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Programs and Services
Privacy

E-mail: pia@state.gov

FY 2008 Privacy Impact Assessment
for
Information Technology Projects

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

(1) Does this system collect, maintain or disseminate personally identifiable information (PII) about individual members of the public?**

YES _X_ NO ___

If the above answer is YES, please complete the survey in its entirety. If NO, complete the certification page and submit the PIA to the following e-mail address: pia@state.gov.

1) Does a Privacy Act system of records already exist?

YES _X_ NO___

If yes, please provide the following:
System Name _Personnel Payroll Records_ **Number** _STATE-30_

If no, a Privacy system of records description will need to be created for this data.

2) What is the purpose of the system/application?
Global Financial Services Charleston Document Imaging System (DIS) transfers information on paper records to electronic form by scanning new submissions as well as existing paper files for current and retired Department of State government employees. The image files will enable accounts managers and technicians to accomplish their tasks faster and without the requirement to move paper files back and forth from storage.

3) What legal authority authorizes the purchase or development of this system/application?

22 U.S.C. 4041; 22 U.S.C. 4071; 22 U.S.C 2651a (Organization of the Department of State); 22 U.S.C. 3921 (Management of Service); and 22 U.S.C. 4042 (Maintenance of the Foreign Service Retirement and Disability Fund)

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

State Department employees, retirees, spouses, dependents, and contractors.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

State Department employees, retirees, their beneficiaries, and contractors are the sources of all information received. State Department employees, retirees, beneficiaries, and contractors when filling out the various required personnel and claims forms can include information on spouses and dependents such as change of address, beneficiary, insurance, SSN, tax ID numbers, date of birth (DOB), age, marital status, and financial banking information.

b. What type of information is collected from the source of the information?

The information relevant to the payroll or transportation claim process on spouses and dependents, such as change of address, beneficiary, insurance SSN, tax ID numbers, date of birth (DOB), age, marital status, and financial banking information.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?
No data is collected from sources other than Department of State records, employees, spouses, dependents, and contractors.

b. How will data be checked for completeness?
Data is currently reviewed for completeness before the forms are processed. For instance, if the form is for a change of beneficiary, the payroll accounts technician verifies that all required information (including signature) has been provided.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).
Data consists of historical records that have been verified and are necessary to complete an information folder for each individual or claim. New data is being imaged immediately after it is collected and verified.

D. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?
Yes, the data is already being collected for use with other Department of State systems. The Document Imaging System replaces the paper copy with an electronic one for processing. Paper copies are still retained for the time period prescribed by the National Archives and Records Administration.

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?
Not applicable. No new data or previously unavailable data will be created.

3) **Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**
Not applicable. No new data or previously unavailable data will be created.

4) **Will the new data be placed in the individual's record?**
Not applicable. No new data will be created by DIS.

5) **How will the new data be verified for relevance and accuracy?**
Not applicable. No new data or previously unavailable data will be created.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**
For various applications within DIS, data will be retrieved by an individual's name, social security number, date of birth, or employee number.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
As addressed in STATE-30, the following are the types of reports that could be produced on individuals: Information consisting of the names, social security numbers, home addresses, dates of birth, dates of hire, quarterly earnings, employer identifying information, and State of hire of employees may be disclosed to the:
- Office of Child Support Enforcement, Administration for Children and Families, Department of Health and Human Services for the purpose of locating individuals to establish paternity, establishing and modifying orders of child support, identifying sources of income, and for other child support enforcement actions as required by the Personal Responsibility and Work Opportunity Reconciliation Act (Welfare Reform Law, 42 U.S.C. 653);
- Office of Child Support Enforcement for release to the Social Security Administration for verifying social security numbers in connection with the operation of the Federal Parent Locator System by the Office of Child Support Enforcement; and
- Office of Child Support Enforcement for release to the Department of Treasury for purposes of administering the Earned Income Tax Credit Program (Section 32, Internal Revenue Code of 1986) and verifying a claim with respect to employment in a tax return.

The principal users of this information outside the Department of State are the:
- Federal, state, and city governments that are issued tax reports;
- Internal Revenue Service and the Social Security Administration who are sent tax and withholding data; and
- Office of Personnel Management who receives the total record of the Civil Service Retirement System and the Federal Employees Retirement System benefit deductions including life and health insurance.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**
Not applicable. The system is being operated in one location only.

2) **What are the retention periods of data in this system?**
The retention periods are as prescribed in Department regulations and National Archives and Records Administration (NARA) guidelines.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**
- Retention of these records varies from 3 to 99 years, depending upon the specific kind of record involved. Records are retired or destroyed in accordance with published records schedules of the Department of State and as approved by the National Archives and Records Administration (NARA).
- More specific information about data retention may be obtained from the Office of Information Programs and Services (A/ISS/IPS).
- Documentation and procedures are maintained by the System Manager: Chief, Applications Programming Division, Systems and Integration Office, Information Management, Bureau of Administration.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
No.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**
Converting from paper to electronic files has no effect on public/employee privacy. The employees and contractors working for the Department have undergone a thorough background security investigation. Access to the Department and its annexes is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals with a proper escort. GFSC has security access controls (code controlled entrances) and/or security alarm systems. All records containing personal information are maintained in secured file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby enabling regular and ad hoc monitoring of computer usage. The system contains personally identifiable information (PII) about employees, spouses, dependents, beneficiaries and contractors.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

The system does not provide the capability to identify, locate, or monitor individuals.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**
STATE-30 is still applicable.

8) **Are there forms associated with the system? YES _X_ NO ___**
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?
Department of State forms are used to conduct business. The forms contain Privacy Act statements that include required information.

F. ACCESS TO DATA:

1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**
Department of State payroll and retirement accounts technicians, claims processors, certifiers, and managers have day-to-day access to the data in the system. GFSC system administrators, information system security officers (ISSOs), and database administrators have access in order to provide application and database support.

2) **What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**
Access procedures identify personnel authorized to use the system. Access control procedures and user responsibilities are documented in the Document Imaging System's System Security Plan.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**
Users' access will be restricted. In accordance with the principle of "Least Privilege," each user has access to only those records in the database for which there is a valid "need to know" in order to accomplish their assigned tasks. The database will be segmented into five separate segments that accessible only to authorized personnel.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)**
Users are accustomed to working with the data in the system. They have undergone background checks and received training in handling personally identifiable information. Annually, users receive cyber-security awareness training given by the Bureau of Diplomatic Security. As noted above, all users will be restricted to browsing only data that they are authorized to view.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**
Contractors are involved in the design and development of the system. The solicitation documents specified security requirements, including the requirement for background investigations. Rules of conduct have been established and contractors have been trained regarding handling of PII under the Privacy Act of 1974, as amended.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**
There will be no direct access to this data by any other system.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**
There will be no direct access to this data by any other agency.